RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART1-R03

SEC Cybersecurity Disclosure Rules: Lessons Learned

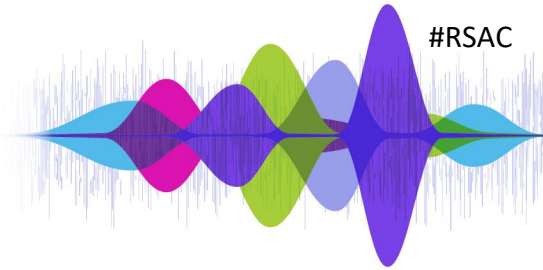
MODERATOR:

Jim Dempsey
Managing Director
Cybersecurity Law Center
IAPP

PANELIST:

Stephen Reynolds
CISSP, CIPP/US
McDermott Will & Emery

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

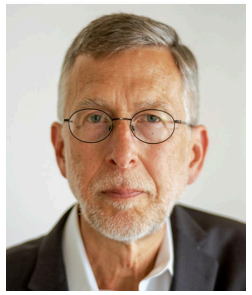
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:



Jim Dempsey

Managing Director
Cybersecurity Law Center,
IAPP

PANELIST:

Stephen Reynolds

CISSP, CIPP/US
Data Security and Privacy Partner
McDermott Will & Emery

RSAC 2025 Conference

Why SEC Reporting Matters

Report, or a Hacker Will Do It For You

ALPHV Blog Collections Api

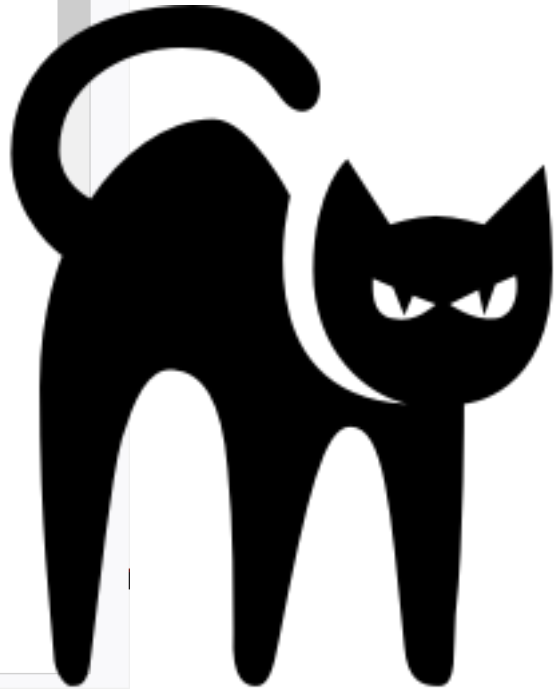
MeridianLink fails to file with the SEC..so we do it for them + 24 hours to pay

11/15/2023, 8:46:42 PM

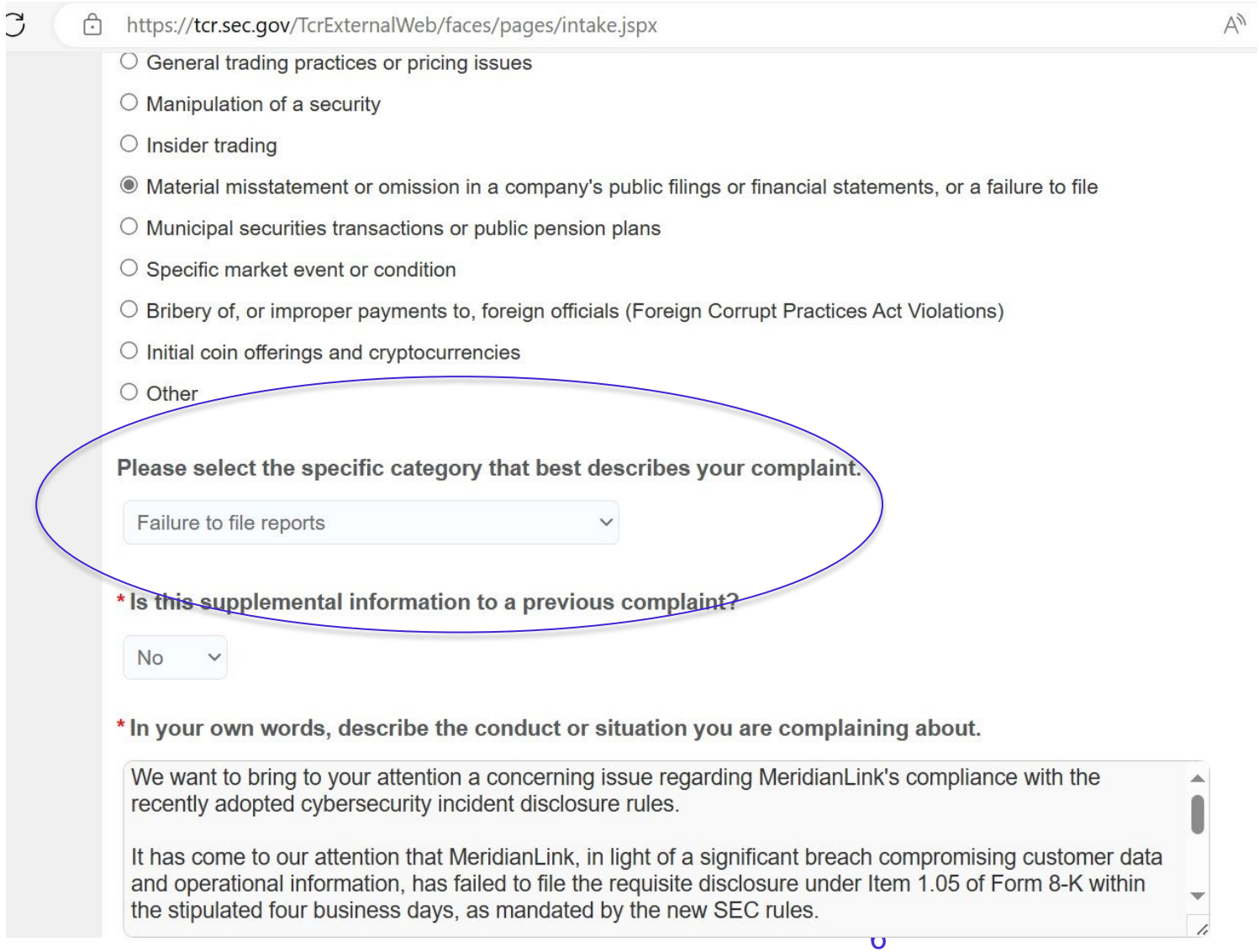
The recent adoption of SEC rules mandates public companies to promptly disclose material cybersecurity incidents under Item 1.05 of Form 8-K within four business days of determining such incidents to be material. Despite this requirement, MeridianLink has not fulfilled this obligation regarding the breach it experienced a week ago. We have therefore reported this non-compliance by MeridianLink, who was involved in a material breach impacting customer data and operational information, for failure to file the required disclosure with the Securities and Exchange Commission (SEC). It appears MeridianLink reached out, but we are yet to receive a message on their end. Maybe this was their DFIR, Mandiant, who did so without authorization from their client. Whatever the reason is.....we are giving you 24 hours before we publish the data in its entirety.

https://tcr.sec.gov/TcrExternalWeb/faces/pages/intake.jspx

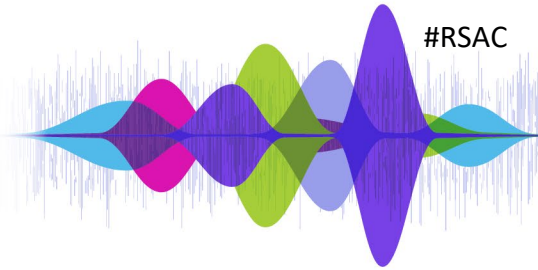
- General trading practices or pricing issues
- Manipulation of a security
- Insider trading



Report, or a Hacker Will Do It For You


https://tcr.sec.gov/TcrExternalWeb/faces/pages/intake.jspx
General trading practices or pricing issues
Manipulation of a security
Insider trading
Material misstatement or omission in a company's public filings or financial statements, or a failure to file
Municipal securities transactions or public pension plans
Specific market event or condition
Bribery of, or improper payments to, foreign officials (Foreign Corrupt Practices Act Violations)
Initial coin offerings and cryptocurrencies
Other
Please select the specific category that best describes your complaint.
Failure to file reports
* Is this supplemental information to a previous complaint?
No
* In your own words, describe the conduct or situation you are complaining about.
We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.
It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

Report, or a Hacker Will Do It For You



"Based on our investigation to date, we have identified no evidence of unauthorized access to our production platforms, and the incident has caused minimal business interruption."

- MeridianLink

RSAC 2025 Conference

Public Disclosures & Press Releases

Many Voices.
One Community.

Disclosing via Press Release

MGM RESORTS UPDATE ON RECENT CYBERSECURITY ISSUE

October 5, 2023

LAS VEGAS, Oct. 5, 2023 /PRNewswire/ -- MGM Resorts International ("MGM Resorts" or the "Company") recently disclosed that the Company identified a cybersecurity issue affecting certain of its systems and that its investigation into the issue was ongoing. On or around September 29, 2023, MGM Resorts determined that an unauthorized third party obtained personal information of some of its customers on September 11, 2023.

The affected information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number. For a limited number of customers, Social Security number and/or passport number was also affected. The types of impacted information varied by individual.

The Company does not believe customer passwords, bank account numbers, or payment card information was affected by this issue.

Disclosing via Press Release

On MGM's 8K Filing, this was their statement (alongside an attached copy of their press release):

- On September 12, 2023, MGM Resorts International (the "Company") issued a press release regarding a cybersecurity issue involving the company.

MGM GRAND
RSAC 2025 Conference

Disclosing via an SEC 8K Filing

Item 8.01 Other Events.

Caesars Entertainment, Inc. (the "Company," "we," or "our") recently identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company. Our customer-facing operations, including our physical properties and our online and mobile gaming applications, have not been impacted by this incident and continue without disruption.

After detecting the suspicious activity, we quickly activated our incident response protocols and implemented a series of containment and remediation measures to reinforce the security of our information technology network. We also launched an investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators. As a result of our investigation, on September 7, 2023, we determined that the unauthorized actor acquired a copy of, among other data, our loyalty program database, which includes driver's license numbers and/or social security numbers for a significant number of members in the database. We are still investigating the extent of any additional personal or otherwise sensitive information contained in the files acquired by the unauthorized actor. We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor.

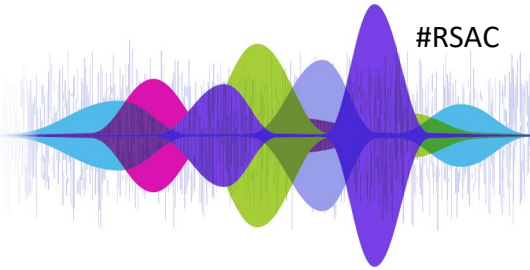
CAESARS PALACE LAS VEGAS

RSAC™ 2025 Conference

SEC Requirements for Cybersecurity Reporting

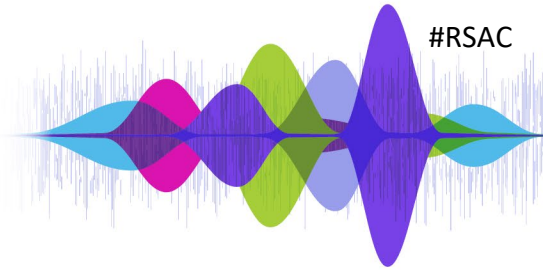
Many Voices.
One Community.

Overview of SEC Reporting Requirements



- Form 8-K Item 1.05 – Material Cybersecurity Incidents
  - Only use after the reporting company has determined incident to be material
- Regulation S-K Item 106
  - Risk management and strategy
    - Process for assessing, identifying and managing material risks
    - Material effects of risks from cybersecurity threats, including previous incidents
  - Governance
    - Board of Directors – oversight of cybersecurity risk
    - Management – assessing and managing material cybersecurity risk
- Other disclosure and reporting requirements (HIPAA, state laws, FTC)

Form 8-K Item 1.05 Disclosure Deadline

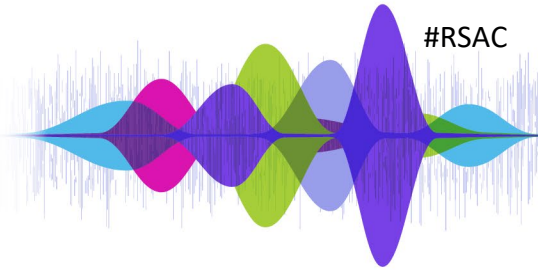


- Form 8-K Reportable Event: Determination that a cybersecurity incident is material
  - “Without unreasonable delay” after discovery of the event
- Disclosure
  - Required within four business days of the materiality determination

RSAC™ 2025 Conference

Making Materiality Determinations

Materiality Standard

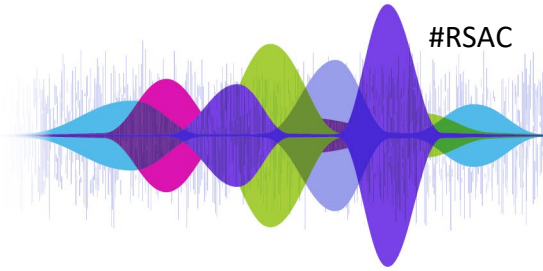


- SEC rules do not provide a specific standard for determining the materiality of a cybersecurity incident
- Materiality should be evaluated based on the total mix of information
- The materiality of a cybersecurity incident depends on whether “there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available”

Materiality Factors

	Quantitative Factors	Qualitative Factors
Short-Term Impact	Remediation costs	Nature and sensitivity of impacted data
	Number of third parties impacted	Scope or nature of harm to third parties
	Amount of impacted data	Impact on key systems and information
	Ransom payments	Risk of litigation and governmental investigation
Long-Term Impact	Lost revenue	Asset and intellectual property loss
	Future availability and/or cost of insurance	Impact of future disclosure of exfiltrated data or intellectual property
	Increased costs of cybersecurity protection and compliance	Reputational and competitive harm
	Other impact on long term financial results	Impact on customer or vendor relationships

Materiality Factors (cont'd)



C&DI Question 104B.05

- Materiality determination required despite payment of ransom and resumption of operations / return of data.
- Companies cannot necessarily conclude that an incident is not material because of prior cessation or apparent cessation of the incident.

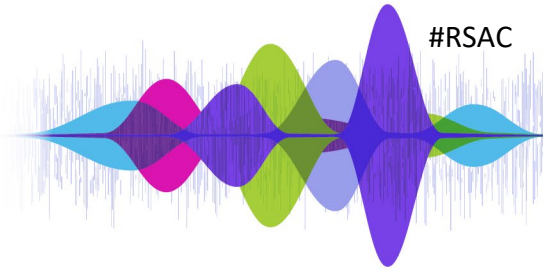
C&DI Question 104B.06

- Disclosure required after materiality determination despite subsequent ransomware payment and cessation the incident

C&DI Question 104B.07

- Availability of insurance coverage does not preclude finding of materiality
- The company should consider both the immediate fallout and any longer-term effects on its operations, finances, brand perception and customer relationships as part of its materiality analysis, including the availability of, or increase in cost of insurance.

Materiality Factors (cont'd)



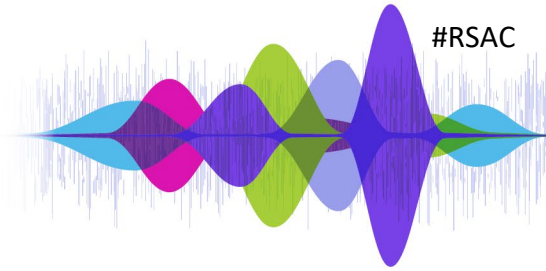
C&DI Question 104B.08:

- Size of any ransomware payment demanded or made is only one of the facts and circumstances to consider in making a materiality determination.
- A lack of quantifiable harm does not preclude a finding of materiality, which also depends on qualitative factors (e.g., reputational harm)

C&DI Question 104B.09

- Series of immaterial but related cybersecurity incidents should be disclosed if they collectively have a material impact on the company. This may be the case where:
  - Same malicious actor engages in small but continuous cyberattacks related in time and form; or
  - Series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business.

Materiality Determination Process



- Failure to timely assess materiality can give rise to liability for disclosure controls and internal controls deficiencies
- Materiality determinations should be contemporaneously documented

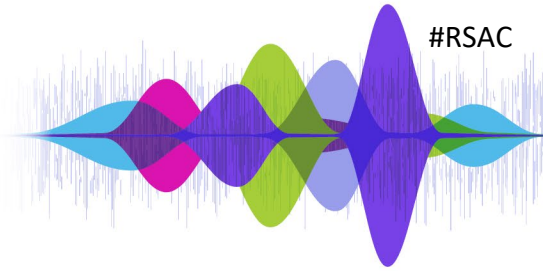
Consider consistency between:

- Response to cybersecurity incident, and
- Form 10k processes for managing cybersecurity risks and board/management roles)

After cybersecurity incident, update disclosures:

- Both material and immaterial cybersecurity incidents should be considered
- Avoid references to actual events as potential risks

Cybersecurity Incidents at Third Parties



Materiality turns on how important a reasonable investor would consider the incident in making an investment decision

- Not contingent on where the relevant electronic systems reside or who owns them
  - Release No. 33-11216: “Reasonable investors would not view a significant breach of a company’s data as immaterial merely because the data were housed on a third-party system”
- Materiality as to the third party is not relevant

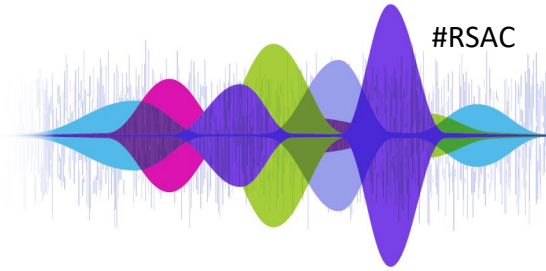
SEC recognizes that public companies have “reduced control” over third-party systems

- Not required to conduct additional inquiries outside regular channels of communication with third-party service providers and in accordance with disclosure controls and procedures

RSAC™ 2025 Conference

Delaying Disclosures

Delays due to national security or public safety

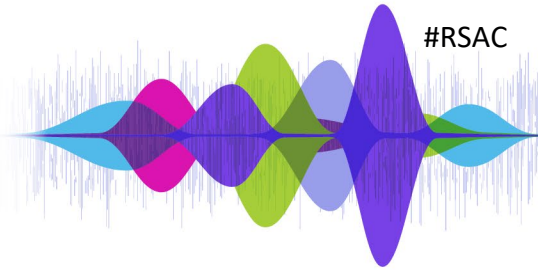


- Public disclosure poses “substantial risk” to national security or public safety
- DOJ guidance on when relief may be granted if:
  - Intended to be granted on a limited basis
  - Most likely if:
    - Method used in the incident is unique and means of mitigation are not known;
    - Incident involves sensitive U.S. government information; or
    - Revealing that the company is aware of incident may undermine remediation.

RSAC 2025 Conference

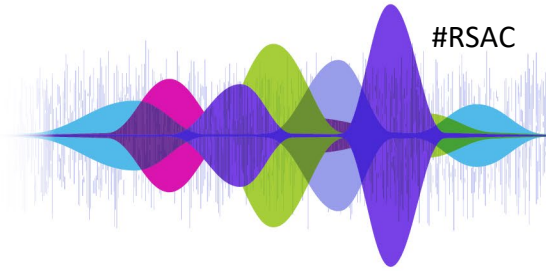
Recent SEC Enforcement Actions

Solarwinds Corporation (Solarwinds) Enforcement Action – Factual Background



- SolarWinds was the victim of a two-year-long cyberattack called “SUNBURST”
  - Internal communications among company personnel show that they knew of several key deficiencies in their cybersecurity practices
    - SolarWinds’ Chief Information Security Officer (CISO) stated on multiple occasions that the remote access set-up was “not very secure”, and a hacker could “basically do whatever without us detecting it until its too late,” and the “current state of security leaves us in a very vulnerable state for our critical assets.”

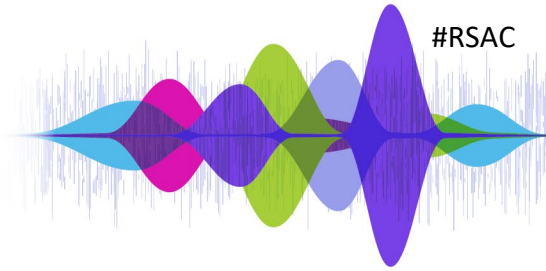
Solarwinds Enforcement Action – Legal Theory



First instance of a public company CISO being charged by the SEC for cybersecurity-related misconduct

First cyber-enforcement action for failure to implement a “system of cybersecurity-related internal accounting controls”

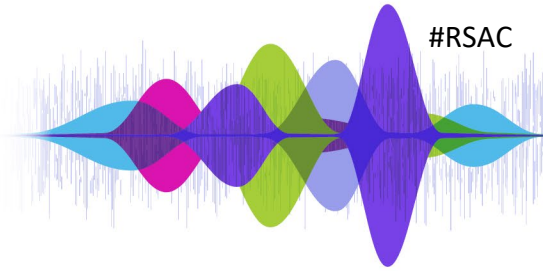
Solarwinds Enforcement Action – The Court's Decision (1/6)



Security Statement made before the breach held to be misleading:

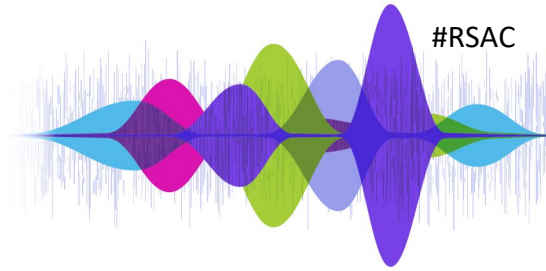
- For example, that statement asserted that SolarWinds had:
  - "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments"
  - "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords"
  - "[a]ccess controls to sensitive data in our databases, systems, and environments [that are] set on a need-to know / least privilege necessary basis." All those statements were materially false and misleading.

Solarwinds Enforcement Action – The Court's Decision (2/6)



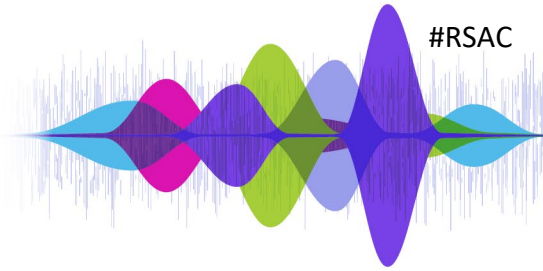
Blogs and press releases before the incident were puffery and lacked detail and thus not actionable.

Solarwinds Enforcement Action – The Court's Decision (3/6)



Cautionary risk disclosures in the company's Form S-1 registration and subsequent periodic Form 10-K, 10-Q, and S-8 filings were adequate.

Solarwinds Enforcement Action – The Court's Decision (4/6)



8-K filed after the incident was adequate - "bluntly reported brutally bad news"-

- "SolarWinds Corporation ("SolarWinds" or the "Company") has been made aware of a cyberattack… SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state, but SolarWinds has not independently verified the identity of the attacker."

Solarwinds Enforcement Action – The Court's Decision (5/6)

Section 13(b)(2)(B)(iii) of the Exchange Act, requiring internal controls, can not be turned into a cybersecurity controls requirement.

Solarwinds Enforcement Action – The Court's Decision (6/6)

Under Exchange Act Rule 13a-15(a), which requires companies to "maintain disclosure controls and procedures," the company's incident response plan was adequate in terms of how it escalated alerts and was adequately followed.

Blackbaud, Inc. Enforcement Action

UNITED STATES OF AMERICA
Before the

III.

2. On July 16, 2020, Blackbaud announced the incident on the company's website and notified the impacted customers. In the website post and notices, the company indicated that the attacker did not access any donor bank account information or social security numbers. Within days of these statements, however, the company's technology and customer relations personnel learned that these claims with respect to bank account information and social security numbers were erroneous. Nevertheless, on August 4, 2020, the company filed a Form 10-Q that discussed the incident, but omitted this material information about the scope of the attack, and misleadingly characterized the risk of exfiltration of such sensitive donor information as hypothetical. At the

3. Based on the foregoing conduct, and the conduct described herein below, Blackbaud violated Sections 17(a)(2) and (3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-13, and 13a-15(a) thereunder.

Blackbaud, Inc. Enforcement Action

Attorney General Todd Rokita secures $49.5 million multistate settlement with Blackbaud for data breach

Attorney General Todd Rokita continued his leadership in the fight to hold tech companies accountable for consumer privacy today, announcing a $49.5 million multistate settlement with the software company, Blackbaud.

“Nonprofits doing their great work rely and depend on vendors like Blackbaud to protect sensitive and private information,” Attorney General Rokita said. “This type of leak is unacceptable, and we fought back on behalf of Hoosiers.”

Attorney General Rokita, with the Attorney General of Vermont, led a coalition of 50 attorneys general to investigate the incident and negotiate a settlement after its d
personal information of millions of co
breach notification practices and also

As lead state, Indiana will receive nea

“While it doesn’t make up for Blackb
General Rokita said.

OFFICE OF THE INDIANA ATTORNEY GENERAL

Under the settlement, Blackbaud has agreed to overhaul its data security and breach notification practices and also make a $49.5 million payment to states.

As lead state, Indiana will receive nearly $3.6 million from the settlement, more than any other state.

RSAC™ 2025 Conference

SEC Compliance Key Takeaways

SEC Declines to Rely on Other Laws/Frameworks

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33-11216;

RIN 3235-AM89

Cybersecurity Risk Mar

AGENCY: Securities and

ACTION: Final rule.

We are also not persuaded that risk quantification or other quantifiable metrics are appropriate as mandatory elements of a cybersecurity disclosure framework. While such metrics may be used by registrants and investors in the future, commenters did not identify any such metrics that would be appropriate to mandate at this time. Additionally, to the extent that a registrant uses any quantitative metrics in assessing or managing cybersecurity risks, it may disclose such information voluntarily. For similar reasons, we decline commenters' recommendations to require disclosure of independent assessments and audits, as well as commenters' recommendations on disclosure of use of the NIST framework, and on distinguishing between continuous and periodic risk assessment.

SEC Compliance Key Takeaways

Incident response procedures should be implemented promptly, including early communications with law enforcement

Disclosure on Form 6-K is not required until a materiality determination has been made, after consultation with external advisors and law enforcement

Materiality determinations should involve careful consideration of quantitative and qualitative factors with contemporaneous documentation of the analysis

When providing disclosure, avoid misleading omissions or facts subject to continuous updates

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

For more information, please contact:

Stephen Reynolds, CISSP, CIPP/US
Tel +1 312 984 3398
Email sreynolds@mwe.com

Jim Dempsey, Managing Director of the IAPP's Cybersecurity Law Center
Email: Jdempsey@iapp.com